How to Create a CC Admin to Access the REST API

https://campus.barracuda.com/doc/79462647/

To use the REST API, each call must be authenticated. For Control Center-managed firewalls, create a dedicated CC admin user and administrative role to allow REST API access. In the administrative role, you can differentiate between the internal and external interface and even grant write permissions to the REST API. Some actions, such as VPN access, may require additional permissions.

Step 1. Create a Custom Administrative Role

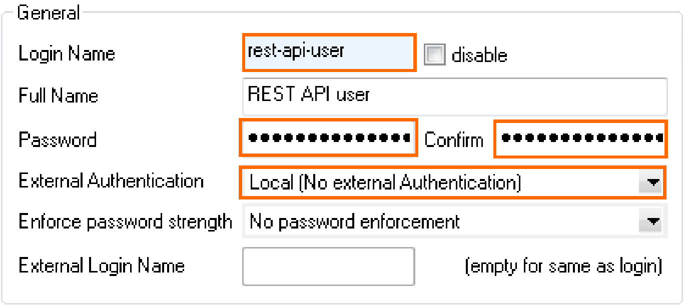
1. Go to **CONFIGURATION** > **Configuration Tree** > **Multi-Range** > **Global Settings** > **Administrative Roles**.
2. Click **Lock**.
3. In the **Roles** section, click **+** to create a new role.
4. Enter a number for the role in the **Name** field and click **OK**. The **Roles** configuration window opens.
5. Enter a **Role Name**.
6. (Optional) Enter a **Description**.
7. Scroll down to add the REST API access rights to the administrative role:
    1. In the **REST API** section, select the **Access to REST API** check box.
    2. Click **Set/ Edit** to configure detailed permissions.
    3. Configure the access rights:
        - **Write Access** – Provides write access on the selected interface.
    4. Click **OK**.
8. Click **OK**.
9. Click **Send Changes** and **Activate**.

Step 2. Create an Admin Account

Add an administrator account, configure authentication settings, and assign the administrative role to the account.

1. Click the **ADMINS** tab.
2. Click **New Entry**.
3. Enter a **Name** for the account. This is the user login name.
4. From the **Range** list, select which ranges the admin should be able to access.
5. From the **Cluster** list, select which clusters that the admin can access.
6. Click **OK**. The **Administrator** configuration window opens.
7. For local authentication, configure username and password:
    - **Login Name** – Enter the username for the REST API CC admin.

- **Full Name** – Enter the full name.
- **Password** – Enter the password.
- **External Authentication** – Select **Local (No external Authentication)**.


General

Login Name: rest-api-user ☐ disable

Full Name: REST API user

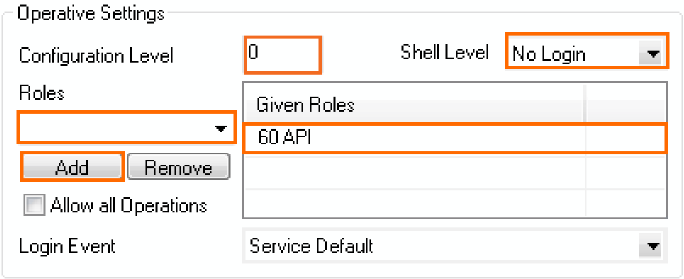
Password: •••••••••••••• Confirm: ••••••••••••••

External Authentication: Local (No external Authentication)

Enforce password strength: No password enforcement

External Login Name: (empty for same as login)

8. Assign the administrative role:
   - **Configuration Level** – Set to `0` to allow write access.
   - **Roles** – Select the role created in Step 1 and click **Add**.
   - **Shell Level** – Select **No Access**.
9. (optional) Change **Login Event** to a less verbose setting.



Operative Settings

Configuration Level: 0

Shell Level: No Login

Roles – Given Roles: 60 API

☐ Allow all Operations

Login Event: Service Default

10. Click **OK**.
11. Click **Activate**.

The CC admin user you just created can now access the REST API interface for the ranges and clusters assigned to the user.

Figures

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.